Sur la paramétrisation des solutions des équations quadratiques

Denis Simon

JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Denis SIMON

Sur la paramétrisation des solutions des équations quadratiques

Tome 18, n° 1 (2006), p. 265-283.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_1_265_0>

Journal de Théorie des Nombres
de Bordeaux **18** (2006), 265-283

Sur la paramétrisation des solutions des équations quadratiques

par Denis SIMON

Résumé. L'objectif de cet article est de proposer un lien entre plusieurs aspects classiques de la théorie des formes quadratiques entières. Dans un premier temps, on étudie en détail les propriétés des formes quadratiques binaires qui paramétrisent les solutions des équations quadratiques ternaires. En particulier, on donne un moyen simple de construire une paramétrisation à partir d'une solution particulière, dont les invariants ne dépendent que de l'équation de départ. Cette paramétrisation permet de simplifier l'algorithme de la 2-descente sur les courbes elliptiques.

Dans un deuxième temps, on considère $Q(X,Y)$ une forme quadratique entière primitive de discriminant Δ non carré. Certains auteurs (dans [1] et [7]) dressent un lien entre une solution rationnelle particulière de $Q(X,Y)=1$ dans $\mathbb{Q}^2$ et une solution de $[R]^2=[Q]$ dans le groupe de classes $Cl(\Delta)$. Nous montrons que ce lien est bien plus direct que celui décrit dans [1] et [7]. En effet, lorsque l'équation $Q(X,Y)=1$ admet une solution, il est possible de paramétrer toutes les solutions sous la forme $X=\frac{q_1(s,t)}{q_3(s,t)}$ et $Y=\frac{q_2(s,t)}{q_3(s,t)}$ où q_1,q_2 et q_3 sont trois formes quadratiques entières avec $\operatorname{Disc} q_3=\Delta$. Nous montrons que la forme quadratique q_3 est exactement (au signe près) la solution R de l'équation $[R]^2=[Q]$ dans $Cl(\Delta)$. Nous comparons alors notre algorithme d'extraction de racine carrée de forme quadratique, avec celui de Gauss.

Abstract. Our goal in this paper is to give a link between different classical aspects of the theory of integral quadratic forms. First, we investigate the properties of the binary quadratic forms involved in the parametrization of the solutions of ternary quadratic equations. In particular, we exhibit a simple rule to obtain a parametrization from a particular solution, such that its invariants only depend on the original equation. Used in the context

Manuscrit reçu le 29 mars 2004.
Mots clefs. Formes quadratiques binaires et ternaires, paramétrisation, groupe de classes.

of elliptic curves, this parametrization simplifies the algorithm of 2-descent.

Secondly, we consider a primitive quadratic form $Q(X, Y)$, with nonsquare discriminant. Some authors (in [1] and [7]) make a link between a particular rational solution of $Q(X, Y) = 1$ over $\mathbb{Q}^2$ and a solution of $[R]^2 = [Q]$ in the class group $Cl(\Delta)$. We explain why this link is much more direct than this. Indeed, when the equation $Q(X, Y) = 1$ has a solution, it is possible to parametrize them all by $X = \frac{q_1(s,t)}{q_3(s,t)}$ and $Y = \frac{q_2(s,t)}{q_3(s,t)}$ where q_1,q_2 and q_3 are three integral quadratic forms with $\mathrm{Disc}\, q_3 = \Delta$. We show that the quadratic form q_3 is exactly (up to sign) the solution R of $[R]^2 = [Q]$ in $Cl(\Delta)$. We end by a comparison between our algorithm for extracting square roots of quadratic forms and the algorithm of Gauss.

Introduction

Lorsqu'une équation quadratique $\mathfrak{Q}(X, Y, Z) = 0$ admet une solution particulière non triviale (X_0, Y_0, Z_0), il est bien connu que l'on peut paramétrer toutes les solutions sous la forme $X = \lambda q_1(s, t)$, $Y = \lambda q_2(s, t)$, $Z = \lambda q_3(s, t)$, où les q_i sont trois formes quadratiques, voir par exemple [12, Ch. IV]. Mais il est moins connu que ces trois formes quadratiques, que l'on construit à partir de la connaissance de (X_0, Y_0, Z_0), peuvent être choisies de telle sorte que leurs discriminants ne dépendent que de $\mathfrak{Q}$, et soient indépendants de (X_0, Y_0, Z_0). Un tel résultat apparaît dans [5] lorsque $\mathfrak{Q}$ est diagonale ou semi-diagonale. Nous montrons, avec le théorème 2.2, que cela reste vrai dans le cas général, et nous donnons un moyen pratique pour les calculer. Remarquons que ce moyen pratique apparaît déjà dans [6, §299], mais sans le calcul de la valeur exacte des discriminants. Comme première application directe, nous montrons que cette paramétrisation, ayant les invariants les plus simples possibles, permet de simplifier sensiblement l'algorithme de la 2-descente sur les courbes elliptiques décrit dans [10].

En appliquant cette paramétrisation au cas particulier des solutions des équations de la forme $AX^2 + BXY + CY^2 = Z^2$, cela nous permet de dresser un lien entre deux aspects très classiques de la théorie des formes quadratiques : la paramétrisation des solutions des équations quadratiques, et le calcul dans le groupe de classes des formes quadratiques.

En effet, soit $Q = AX^2 + BXY + CY^2$ une forme quadratique entière primitive de discriminant $\Delta = B^2 - 4AC$. Nous supposerons toujours que l'entier Δ est non carré (et donc non nul). Grâce à la composition de Gauss, les formes quadratiques primitives de discriminant Δ, modulo équivalence pour l'action de $SL_2(\mathbb{Z})$, forment un groupe fini $Cl(\Delta)$ (voir par exemple [2, Ch. 14]). On note $[Q]$ la classe d'équivalence de Q. Par définition, la

forme Q est dans le genre principal si elle représente 1, partout localement, c'est-à-dire si l'équation $Q(X,Y) = 1$ admet une solution p-adique dans $\mathbb{Z}_p^2$, pour tout p, ainsi que dans $\mathbb{R}^2$. Dans [2, §14.3] on trouve une preuve du théorème suivant :

Théorème (Gauss)**.** *Le genre principal est exactement* $Cl(\Delta)^2$.

L'existence de solutions entières locales implique en particulier l'existence de solutions rationnelles locales, et donc d'après le Principe de Hasse, l'existence de solutions globales dans $\mathbb{Q}^2$. Ainsi, on voit que si l'équation $[R]^2 = [Q]$ a une solution dans $Cl(\Delta)$, alors l'équation $Q(X,Y) = 1$ a une solution dans $\mathbb{Q}^2$. Si l'on tient compte aussi des solutions entières locales, ceci devient une équivalence. Ce résultat est rendu explicite dans [1] et [7], où la forme quadratique R est construite à partir d'une solution particulière de $Q(X,Y) = 1$. Nous voulons montrer que le lien n'est pas naturellement entre R et la solution particulière, mais entre R et la paramétrisation des solutions.

On sait aussi que lorsque l'équation $Q(X,Y) = 1$ admet une solution rationnelle, elle en admet une infinité, que l'on peut paramétrer sous la forme

$$X = \frac{q_1(s,t)}{q_3(s,t)} \quad Y = \frac{q_2(s,t)}{q_3(s,t)}\,,$$

où q_1,q_2 et q_3 sont des formes quadratiques. D'après le théorème 2.2, ou [5], on peut même s'arranger pour que le discriminant de q_3 soit exactement Δ.

Notre objectif est de faire le lien entre la forme quadratique R satisfaisant $[R]^2 = [Q]$ dans $Cl(\Delta)$ et la forme quadratique q_3 de discriminant Δ issue de la paramétrisation des solutions de $Q(X,Y) = 1$:

Théorème. *Soient Q et q_3 deux formes quadratiques entières primitives de discriminant Δ (non carré). Les propositions suivantes sont équivalentes :*

(i) on a $[q_3]^2 = [Q]^{\pm 1}$ dans $Cl(\Delta)$,

(ii) on peut trouver deux formes quadratiques entières $q_1(s,t)$ et $q_2(s,t)$ telles que les solutions de $Q(X,Y) = 1$ soient paramétrées par $X = \dfrac{q_1(s,t)}{q_3(s,t)}$ et $Y = \dfrac{q_2(s,t)}{q_3(s,t)}$.

La forme quadratique q_3, issue de la paramétrisation, n'est pas nécessairement primitive, en particulier lorsque $Q(X,Y) = 1$ admet une solution rationnelle p-adique, mais pas de solution entière p-adique. Cela ne peut arriver que lorsque Δ est divisible par p^2. Nous donnons un critère sur la solution particulière utilisée pour la construction de q_3, pour décider si q_3 est primitive. En particulier, lorsque Δ est un discriminant fondamental, q_3 est toujours primitive.

Nous obtenons ainsi un algorithme pour la résolution de $[R]^2 = [Q]$ dans $Cl(\Delta)$, qui consiste simplement à chercher une solution particulière de $Q(X,Y) = 1$, puis une paramétrisation de toutes les solutions. En comparant à l'algorithme de Gauss (voir [6, §286], [9] ou [8]), on voit que ces deux algorithmes sont essentiellement équivalents. Le théorème 4.3 nous permet donc de proposer une nouvelle interprétation de l'algorithme assez technique de Gauss, pour la recherche d'une racine carrée dans le groupe de classes, en termes de la paramétrisation, beaucoup plus classique, des solutions des équations quadratiques.

1. Propriétés des solutions paramétriques des formes quadratiques ternaires

Dans toute cette partie, on travaille sur un corps K de caractéristique différente de 2.

Notation. On note $\mathfrak{Q}$ une forme quadratique ternaire, définie sur K. On note aussi $\mathfrak{Q}$ la matrice de la forme bilinéaire associée à $\mathfrak{Q}$. On note $q_i(s,t) = q_{i,1}s^2 + q_{i,2}st + q_{i,3}t^2$ pour $i = 1,2,3$ trois formes quadratiques binaires à coefficients dans K, et q la matrice 3×3 dont les coefficients sont $q_{i,j}$. Pour toute matrice M d'ordre 3×3, on note M^* sa matrice adjointe, de sorte que $MM^* = M^*M = (\det M)Id_3$. On note enfin $\mathfrak{Q}_0 = \begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}$. Cette matrice correspond à la forme quadratique $x_2^2 - x_1x_3$.

Lemme 1.1. *On a $\mathfrak{Q}(q_1,q_2,q_3) = 0$ si et seulement si $q^t\mathfrak{Q}q = \lambda\mathfrak{Q}_0$ pour un certain $\lambda \in K$.*

Démonstration. Par définition, la relation $\mathfrak{Q}(q_1,q_2,q_3) = 0$ équivaut à

$$\begin{pmatrix} s^2 & st & t^2 \end{pmatrix} q^t\mathfrak{Q}q \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix} = 0.$$

Or, les matrices M qui satisfont $\begin{pmatrix} s^2 & st & t^2 \end{pmatrix} M \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix} = 0$ sont nécessairement proportionnelles à $\mathfrak{Q}_0$, d'où le lemme. La réciproque est immédiate. □

Lemme 1.2. *Si $\mathfrak{Q}(q_1,q_2,q_3) = 0$ avec $\det\mathfrak{Q} \neq 0$, alors $\mathrm{Rang}(q) \neq 2$.*

Démonstration. On a $q^t\mathfrak{Q}q = \lambda\mathfrak{Q}_0$ avec $\lambda \in K$. Si $\mathrm{Rang}(q) < 3$, alors $\lambda = 0$. Mais on a alors $\mathrm{Im}(\mathfrak{Q}q) \subset \ker(q^t)$, et donc $\mathrm{Rang}(\mathfrak{Q}q) \leqslant \dim ker(q)$. De plus, $\dim ker(q) = 3 - \mathrm{Rang}(q)$, et comme $\mathfrak{Q}$ est inversible, on a $\mathrm{Rang}(\mathfrak{Q}q) = \mathrm{Rang}(q)$. De là, on déduit $\mathrm{Rang}(q) \leqslant \frac{3}{2}$, donc $\mathrm{Rang}(q) \leqslant 1$. □

Proposition 1.3. *Supposons que* $\mathfrak{Q}(q_1, q_2, q_3) = 0$ *avec* $\det \mathfrak{Q} \neq 0$.

(i) Si $\mathrm{Rang}(q) > 1$, *alors* $\mathrm{Rang}(q) = 3$ *et* (q_1, q_2, q_3) *paramétrise toutes les solutions de* $\mathfrak{Q}(x_1, x_2, x_3) = 0$ *dans* $\mathbb{P}^2(K)$;

(ii) Si $\mathrm{Rang}(q) = 1$, *alors* (q_1, q_2, q_3) *ne représente qu'un seul point dans* $\mathbb{P}^2(K)$;

(iii) Si $\mathrm{Rang}(q) = 0$, *alors* $(q_1, q_2, q_3) = (0, 0, 0)$.

Démonstration. Seul le point (i) n'est pas trivial. D'après les lemmes 1.1 et 1.2, on a $q^t \mathfrak{Q} q = \lambda \mathfrak{Q}_0$ avec $\lambda \neq 0$. En particulier, $\det q \neq 0$. On a $\mathfrak{Q} = \lambda (q^{-1})^t \mathfrak{Q}_0 q^{-1}$. Soit X_0 une solution particulière non triviale de $X_0^t \mathfrak{Q} X_0 = 0$. On a $(q^{-1}X_0)^t \mathfrak{Q}_0 (q^{-1}X_0) = 0$. Mais on sait que les solutions de $Y^t \mathfrak{Q}_0 Y = 0$ sont de la forme $Y = \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}$. On a donc $X_0 = qY = \begin{pmatrix} q_1(s,t) \\ q_2(s,t) \\ q_3(s,t) \end{pmatrix}$. □

Proposition 1.4. *On suppose que* $\mathfrak{Q}(q_1, q_2, q_3) = 0$ *avec* $\det \mathfrak{Q} \neq 0$ *et* $\mathrm{Rang}(q) > 1$. *Alors il existe* $\mu \neq 0$ *tel que*

(i)	$q^t \mathfrak{Q} q = (-4 \det \mathfrak{Q})\ \mu^2 \mathfrak{Q}_0$		
(ii)	$\det q = (-4 \det \mathfrak{Q})\ \mu^3$		
(iii)	$\mathrm{Disc}\, q_i = (-4 \mathfrak{Q}^*_{i,i})\ \mu^2$		*pour* $i \in \{1,2,3\}$
(iv)	$\mathrm{Res}(q_i, q_j) = (-4 \det \mathfrak{Q})\ \mathfrak{Q}_{k,k}\ \mu^4$		*pour* i, j, k *deux à deux distincts.*

Démonstration. D'après les lemmes 1.1 et 1.2, on a $q^t \mathfrak{Q} q = \lambda \mathfrak{Q}_0$ avec $\lambda \neq 0$. On déduit en particulier que $-4 \det \mathfrak{Q} (\det q)^2 = \lambda^3$. Posons $\lambda = (-4 \det \mathfrak{Q}) \lambda'$, avec $\lambda' \neq 0$. On trouve $(\det q)^2 = (-4 \det \mathfrak{Q})^2 \lambda'^3$. Cette relation implique que λ' est un carré, disons $\lambda' = \mu^2$. On a donc la relation (i). En choisissant convenablement le signe de μ, on obtient (ii). Les autres relations sont des conséquences directes de la relation (i). Par exemple, les discriminants $\mathrm{Disc}\, q_i = q_{i,2}^2 - 4 q_{i,1} q_{i,3}$ sont donnés formellement par $(q \mathfrak{Q}_0^{-1} q^t)_{i,i}$. En inversant la relation (i), on trouve $q \mathfrak{Q}_0^{-1} q^t = (-4 \det \mathfrak{Q}) \mu^2 \mathfrak{Q}^{-1} = -4 \mu^2 \mathfrak{Q}^*$, d'où la relation (iii). De même, les résultants $\mathrm{Res}(q_i, q_j)$ sont donnés formellement par $\mathrm{Res}(q_i, q_j) = (q^{*t} \mathfrak{Q}_0 q^*)_{k,k}$, où i, j et k sont deux à deux distincts. En multipliant (i) à gauche par q^{*t} et à droite par q^*, on trouve $q^{*t} \mathfrak{Q}_0 q^* = (-4 \det \mathfrak{Q}) \mu^4 \mathfrak{Q}$, d'où la relation (iv). □

2. Construction d'une paramétrisation entière à partir d'une solution particulière

Notation. On note $Sym_3(\mathbb{Z})$ l'ensemble des matrices symétriques 3×3 à coefficients diagonaux dans $\mathbb{Z}$ et non diagonaux dans $\frac{1}{2}\mathbb{Z}$. Ces matrices sont naturellement en bijection avec les formes quadratiques ternaires à coefficients entiers. En particulier, si $\mathfrak{Q} \in Sym_3(\mathbb{Z})$, on a $4\mathfrak{Q}^* \in \mathcal{M}_3(\mathbb{Z})$, et $4 \det \mathfrak{Q} \in \mathbb{Z}$.

Le théorème suivant montre qu'il est possible de construire une paramétrisation des solutions d'une équation quadratique ternaire ayant de bons invariants à partir d'une solution particulière quelconque. Il généralise le résultat donné dans [5]. On commence par donner une construction simple dans le cas où $(1,0,0)$ est une solution particulière. La construction est analogue à celle donnée dans [6, §299].

Lemme 2.1. *On suppose que* $\mathfrak{Q}$ *est de la forme* $\mathfrak{Q} = \begin{pmatrix} 0 & \frac{a}{2} & \frac{b}{2} \\ \frac{a}{2} & c & \frac{d}{2} \\ \frac{b}{2} & \frac{d}{2} & e \end{pmatrix}$. *Soit* $\widehat{\mathfrak{Q}} = \begin{pmatrix} c & d & e \\ -a & -b & 0 \\ 0 & -a & -b \end{pmatrix}$. *On a* $\det \widehat{\mathfrak{Q}} = -4 \det \mathfrak{Q}$ *et* $\widehat{\mathfrak{Q}}^t \mathfrak{Q} \widehat{\mathfrak{Q}} = (-4 \det \mathfrak{Q}) \mathfrak{Q}_0$.

Démonstration. On a $-4 \det \mathfrak{Q} = ea^2 - dab + cb^2$. La vérification des formules est immédiate. □

Théorème 2.2. *Soit* $\mathfrak{Q} \in Sym_3(\mathbb{Z})$ *avec* $\det \mathfrak{Q} \neq 0$. *On suppose que l'équation* $X^t \mathfrak{Q} X = 0$ *admet une solution* $X_0 \in \mathbb{Q}^3$ *non triviale. On peut paramétrer les solutions de* $\mathfrak{Q}(x_1, x_2, x_3) = 0$ *dans* $\mathbb{P}^2(\mathbb{Q})$ *par* $q = (q_1, q_2, q_3)$, *où les* q_i *sont trois formes quadratiques entières telles que*

$$\begin{array}{lrll} (i) & q^t \mathfrak{Q} q = & (-4 \det \mathfrak{Q})\ \mathfrak{Q}_0 & \\ (ii) & \det q = & (-4 \det \mathfrak{Q}) & \\ (iii) & \operatorname{Disc} q_i = & (-4 \mathfrak{Q}^*_{i,i}) & \text{pour } i \in \{1,2,3\} \\ (iv) & \operatorname{Res}(q_i, q_j) = & (-4 \det \mathfrak{Q})\ \mathfrak{Q}_{k,k} & \text{pour } i,j,k \text{ deux à deux distincts.} \end{array}$$

Démonstration. On donne une démonstration constructive de ce résultat. On veut se ramener à la situation de lemme 2.1. Quitte à multiplier X_0 par un rationnel convenable, on peut supposer que les coefficients de X_0 sont entiers et premiers entre eux. Construisons une matrice M de taille 3×3 de déterminant 1 et dont la première colonne soit X_0. En utilisant la forme normale d'Hermite de X_0^t, on trouve une matrice $U \in SL_3(\mathbb{Z})$ telle que $X_0^t U^t = (1,0,0)$. La matrice $M = U^{-1}$ a les propriétés requises.

Soit $\mathfrak{Q}' = M^t \mathfrak{Q} M \in Sym_3(\mathbb{Z})$. On peut appliquer le lemme 2.1 à $\mathfrak{Q}'$. On a alors $\widehat{\mathfrak{Q}'} \in \mathcal{M}_3(\mathbb{Z})$ avec $\det \widehat{\mathfrak{Q}'} = -4 \det \mathfrak{Q}$ et $\widehat{\mathfrak{Q}'}^t \mathfrak{Q}' \widehat{\mathfrak{Q}'} = (-4 \det \mathfrak{Q}) \mathfrak{Q}_0$. En posant $q = M \widehat{\mathfrak{Q}'}$, on a $q \in \mathcal{M}_3(\mathbb{Z})$ avec $\det q = -4 \det \mathfrak{Q}$ et $q^t \mathfrak{Q} q = (-4 \det \mathfrak{Q}) \mathfrak{Q}_0$.

On définit les formes quadratiques q_i par les coefficients de la matrice q. Comme les coefficients de q sont entiers, les formes quadratiques sont entières. D'après le lemme 1.1, on a $\mathfrak{Q}(q_1, q_2, q_3) = 0$. De plus, $\det q = -4 \det \mathfrak{Q} \neq 0$, donc la proposition 1.4 est vérifiée avec $\mu = 1$. Enfin, la proposition 1.3 montre que (q_1, q_2, q_3) paramétrise toutes les solutions de $\mathfrak{Q}(x_1, x_2, x_3) = 0$ dans $\mathbb{P}^2(\mathbb{Q})$. □

Remarque. Dans cette construction, si on prend une matrice M quelconque dont la première colonne est X_0, la proposition 1.4 est vérifiée avec $\mu = \det M$. En particulier, si la solution particulière est (x_1, x_2, x_3) la construction la plus classique revient à prendre $M = \begin{pmatrix} x_1 & 0 & 1 \\ x_2 & 1 & 0 \\ x_3 & 0 & 0 \end{pmatrix}$, dont le déterminant est $-x_3$.

Corollaire 2.3. *Soient $A, B, C, D \in \mathbb{Z}$ et $\Delta = B^2 - 4AC$. On suppose que $D\Delta \neq 0$ (Δ peut éventuellement être carré). Si l'équation $AX^2 + BXY + CY^2 = DZ^2$ admet une solution non triviale sur $\mathbb{Q}$, alors on peut trouver une paramétrisation des solutions de la forme $X = u{\cdot}q_1(s,t)$, $Y = u{\cdot}q_2(s,t)$, $Z = u \cdot q_3(s,t)$, avec $u \in \mathbb{Q}$, de sorte que q_1, q_2, et q_3 sont trois formes quadratiques entières satisfaisant*

$$\begin{aligned} \operatorname{Disc} q_1 &= 4CD \\ \operatorname{Disc} q_2 &= 4AD \\ \operatorname{Disc} q_3 &= \Delta \\ \operatorname{Res}(q_1, q_2) &= D^2\Delta \\ \operatorname{Res}(q_1, q_3) &= -CD\Delta \\ \operatorname{Res}(q_2, q_3) &= -AD\Delta \\ \det q &= -D\Delta \end{aligned}$$

Démonstration. On applique les résultats précédents à la matrice $\mathfrak{Q} = \begin{pmatrix} A & \frac{B}{2} & 0 \\ \frac{B}{2} & C & 0 \\ 0 & 0 & -D \end{pmatrix}$. □

On retrouve dans ce cas le résultat de [5], mais la construction est différente.

Comme les discriminants des formes quadratiques q_1 et q_2 sont pairs, on remarque que leurs coefficients centraux sont pairs.

3. Application du théorème 2.2 aux courbes elliptiques

On a vu dans [11] comment résoudre efficacement les équations quadratiques qui apparaissent dans l'algorithme de la 2–descente pour les courbes elliptiques définies sur $\mathbb{Q}$ tel qu'il est proposé dans [10]. Nous proposons ici de paramétrer les solutions de cette équation, en utilisant le théorème 2.2 plutôt que la paramétrisation donnée dans [10]. Le gain est immédiat, puisque les invariants du polynôme quartique que l'on construit ensuite sont nettement plus petits.

Plus précisément, la 2–descente peut se décrire de la manière suivante. On considère la courbe elliptique $E : ky^2 = x^3 + Ax^2 + Bx + C$, où le polynôme $P(x) = x^3 + Ax^2 + Bx + C$ est supposé à coefficients entiers

et irréductible sur $\mathbb{Q}$. Soit θ une racine de P et K le corps $K = \mathbb{Q}(\theta)$. Si la courbe possède un point non trivial de coordonnées rationnelles (x, y), on peut écrire $ky^2 = \mathcal{N}_{K/\mathbb{Q}}(x - \theta)$. En pratique on ne connaît ni x ni y et l'algorithme de la 2–descente a justement pour objectif final de les retrouver. On peut toutefois montrer que le nombre algébrique $\delta = k(x - \theta)$ ne peut prendre qu'un nombre fini de valeurs dans K^*/K^{*2} (voir [10, prop. 1.4]). En particulier, la valuation de δ en tout idéal premier $\mathfrak{P}$ de K est paire, sauf peut–être si $\mathfrak{P}$ est au dessus d'un nombre premier p divisant k ou dont le carré divise $\mathrm{Disc}\, P$. Ceci signifie que δ est égal, à un carré près, à une S–unité, pour un ensemble S d'idéaux premiers tout à fait explicite et ne dépendant que de k et de P.

Bien entendu, toutes les S–unités, même à un carré près, ne sont pas de la forme $k(x - \theta)$, c'est-à-dire sans coefficient en θ^2 et avec un coefficient en θ égal à $-k$ (à un carré de $\mathbb{Q}$ près). Notons donc $\delta = a - b\theta + c\theta^2 \in K^*$ une S–unité connue, avec a,b et c trois entiers. On cherche alors $z \in K^*$ de la forme $z = u + v\theta + w\theta^2$ tel que δz^2 soit de la forme $k(a' - y^2\theta)$, avec $y, a' \in \mathbb{Q}$. En écrivant

$$\delta z^2 = q_0(u, v, w) - q_1(u, v, w)\theta + q_2(u, v, w)\theta^2 \ ,$$

où les q_i sont des formes quadratiques à coefficients dans $\mathbb{Z}$ en les variables u, v, w, on voit qu'il faut résoudre simultanément

$$\begin{cases} q_2(u, v, w) = 0 \\ q_1(u, v, w) = ky^2 \end{cases}$$

En utilisant l'algorithme de résolution des équations quadratiques décrit dans [11], on peut trouver une solution particulière $X_0 = (u_0, v_0, w_0)$ de la première équation. En effet, ceci ne requiert que la factorisation de $\det q_2$, or il se trouve que celui–ci est égal à $-\mathcal{N}_{K/\mathbb{Q}}(\delta)$, ce qui signifie que c'est une S–unité, donc $\det q_2$ est facile à factoriser. L'étape suivante consiste à paramétrer les solutions de $q_2(u, v, w) = 0$ par des formes quadratiques $u(s, t)$, $v(s, t)$ et $w(s, t)$, puis de substituer ces expressions dans la deuxième équation $q_1(u, v, w) = ky^2$, où l'on voit donc apparaître une quartique.

Rappelons que les invariants d'un polynôme quartique $Q = ax^4 + bx^3 + cx^2 + dx + e$ sont $I = 12ae - 3bd + c^2$, $J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$ et $27\,\mathrm{Disc} = 4I^3 - J^2$. Si l'on voit P comme un polynôme de degré 4 dont le coefficient en x^4 est nul, on a a priori deux notions de discriminant pour P. Ces deux notions diffèrent en général d'un facteur l^2, où l est le coefficient de degré 3 de P. Ici, $l = 1$, donc les deux notions sont identiques.

Si l'on suit la paramétrisation donnée dans [10], la quartique obtenue est de la forme

$$4b^3ky^2 = Q(s, t) \ ,$$

où $b = q_1(X_0)$ et $Q(s,t)$ est un polynôme dont les invariants sont $\operatorname{Disc} Q = 2^{12}b^6 \operatorname{Disc} P$, $I(Q) = 2^4 b^2 I(P)$ et $J(Q) = 2^6 b^3 J(P)$. On voit donc apparaître le facteur parasite b, qui dépend de la solution particulière trouvée, et qui n'a aucune raison d'être ni petit, ni simplement factorisable. Une étape de minimisation est nécessaire pour le faire disparaître.

Montrons qu'en utilisant la paramétrisation donnée par le théorème 2.2, on trouve des invariants plus simples et, surtout, indépendants de la solution particulière X_0.

Soit $X = qV$ une paramétrisation donnée par le théorème 2.2 à partir de la solution particulière X_0, où l'on note encore $V = \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}$. En remplaçant dans l'équation $q_1 = ky^2$, on obtient l'équation

$$Q(s,t) = ky^2 \ ,$$

où $Q(s,t) = X^t q_1 X = V^t (q^t q_1 q) V$. Il reste à étudier les invariants du polynôme quartique Q. On remarque d'abord que Q est défini à partir de la matrice $q^t q_1 q$, donc ses coefficients sont entiers. Il pourrait tout aussi bien être défini par $q^t q_1 q + \lambda \mathfrak{Q}_0$ pour n'importe quelle valeur de λ, puisque $V^t \mathfrak{Q}_0 V = 0$. Ainsi, les invariants de Q doivent pouvoir encore se lire sur cette nouvelle matrice, et rester toutefois indépendants de λ. On a le résultat suivant :

Lemme 3.1. *Soit $\mathfrak{Q}$ une matrice 3×3 symétrique. On considère les deux polynômes quartiques $Q(s,t) = V^t \mathfrak{Q} V$ et $Q'(s,t) = -s \det(s\mathfrak{Q} + 2t\mathfrak{Q}_0)$. Alors Q et Q' ont les mêmes invariants I, J et* Disc.

Démonstration. C'est un calcul formel élémentaire laissé au lecteur. □

Ainsi, les invariants de Q sont les mêmes que ceux de $Q' = -s \det(sq^t q_1 q + 2t\mathfrak{Q}_0)$. D'après le théorème 2.2, on a $\det q = -4 \det q_2 = 4\mathcal{N}_{K/\mathbb{Q}}(\delta)$ et $q^t q_2 q = 4\mathcal{N}_{K/\mathbb{Q}}(\delta)\mathfrak{Q}_0$. On a alors

$$\begin{aligned} Q' &= -s \det(sq^t q_1 q + 2t\mathfrak{Q}_0) \\ &= -s \det\left(sq^t q_1 q + \tfrac{2t}{4\mathcal{N}_{K/\mathbb{Q}}(\delta)} q^t q_2 q\right) \\ &= -s 2^4 \mathcal{N}_{K/\mathbb{Q}}(\delta)^2 \det\left(sq_1 + \tfrac{2t}{4\mathcal{N}_{K/\mathbb{Q}}(\delta)} q_2\right) \end{aligned}$$

Or, on a aussi la relation

$$\det(sq_1 + tq_2) = -\mathcal{N}_{K/\mathbb{Q}}(\delta) s^3 P\left(\frac{t}{s} - A\right) \ ,$$

donc

$$Q' = s^4 2^4 \mathcal{N}_{K/\mathbb{Q}}(\delta)^3 P\left(\frac{2t}{4\mathcal{N}_{K/\mathbb{Q}}(\delta) s} - A\right) \ .$$

À partir de là, on peut exprimer les invariants de Q' en fonction de ceux de P. En utilisant le lemme 3.1, on trouve finalement :

$$\begin{aligned} I(Q) &= 2^4 \mathcal{N}_{K/\mathbb{Q}}(\delta)^2 I(P) \\ J(Q) &= 2^6 \mathcal{N}_{K/\mathbb{Q}}(\delta)^3 J(P) \\ \operatorname{Disc} Q &= 2^{12} \mathcal{N}_{K/\mathbb{Q}}(\delta)^6 \operatorname{Disc} P \end{aligned}$$

4. Application du théorème 2.2 au calcul de la racine carrée d'une forme quadratique

Soit Δ un discriminant quadratique (non carré). Le théorème principal annoncé dans l'introduction peut paraître surprenant par le lien qu'il fait entre deux théories apparemment disjointes. Il devient beaucoup plus naturel si l'on se souvient qu'il existe plusieurs descriptions différentes du groupe de classes $Cl(\Delta)$. Commençons donc par rappeler les différentes définitions pour la loi de composition des formes quadratiques et pour le groupe $Cl(\Delta)$. On pourra aussi voir [4, §I.3], [3, §5.2] ou [1, §2] pour une comparaison entre ces définitions.

Historiquement, la première est celle de Gauss ([6, §235]) et est définie de la manière suivante : grâce à la théorie de la réduction, on montre d'abord qu'il n'y a qu'un nombre fini de classes de formes quadratiques entières primitives de discriminant Δ pour l'action de $SL_2(\mathbb{Z})$: $Q(s,t) = as^2 + bst + ct^2 \mapsto Q(\alpha s + \beta t, \gamma s + \delta t)$; on note $\mathcal{F}(\Delta)$ cet ensemble fini ; si $Q_i = a_i s^2 + b_i st + c_i t^2 \in \mathcal{F}(\Delta)$ pour $i \in \{1,2,3\}$, on dit que Q_3 est la composition de Q_1 et Q_2 si l'on a une relation de la forme

$$Q_1(s_1,t_1) Q_2(s_2,t_2) = Q_3(s_3,t_3)$$

avec

$$\begin{cases} s_3 = x_1 s_1 s_2 + x_2 s_1 t_2 + x_3 t_1 s_2 + x_4 t_1 t_2 \\ t_3 = y_1 s_1 s_2 + y_2 s_1 t_2 + y_3 t_1 s_2 + y_4 t_1 t_2 \end{cases}$$

où les x_i et y_i sont des entiers satisfaisant les relations

$$\begin{aligned} x_1 y_2 - y_1 x_2 &= a_1 \\ x_1 y_3 - y_1 x_3 &= a_2 \end{aligned}$$

(ces dernières relations étant appelées conditions d'orientation). Muni de cette loi, $\mathcal{F}(\Delta)$ est un groupe abélien fini. Cette définition de la composition des formes quadratiques a l'avantage d'être à la fois concrète et relativement naturelle, mais elle s'avère assez lourde à manipuler.

Dirichlet a ensuite montré que cette composition dans $\mathcal{F}(\Delta)$ est équivalente à une autre forme bien plus explicite (voir [4, prop. I.3.8] et [3, 5.4.6]) : les coefficients de Q_3 sont donnés par les formules

$$a_3 = \frac{a_1 a_2}{d^2} \; ; \quad b_3 = b_2 + 2\frac{a_2}{d}\left(\lambda \frac{b_1 - b_2}{2} - \nu c_2\right) \; ; \quad c_3 = \frac{b_3^2 - \Delta}{4a_3}$$

avec

$$d = pgcd\left(a_1, a_2, \frac{b_1+b_2}{2}\right) = \lambda a_1 + \mu a_2 + \nu\frac{b_1+b_2}{2} ,$$

(le choix des entiers λ, μ et ν n'est pas unique, mais toutes les formes ainsi obtenues sont équivalentes). La composition des formes ainsi décrite est beaucoup plus adaptée au calcul, en particulier sur ordinateur. Ces formules peuvent même servir de définition pour la composition. Malheureusement, elles occultent complètement l'intuition qui était à l'origine de la définition de Gauss.

Un point de vue plus moderne consiste à associer à toute forme quadratique primitive de discriminant Δ un idéal dans l'ordre quadratique $\mathbb{Z}_\Delta$ de discriminant Δ :

$$as^2 + bst + ct^2 \mapsto \left(a\mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2}\mathbb{Z}\right)\sqrt{\Delta}^{(1-signe(a))/2}$$

(la puissance de Δ dans cette expression est ici encore une condition d'orientation). Cette application définit une bijection entre l'ensemble $\mathcal{F}(\Delta)$ et le groupe de classes $Cl(\Delta)$, quotient du groupe des idéaux fractionnaires inversibles par le sous–groupe engendré par les éléments *totalement positifs* de $\mathbb{Q}(\sqrt{\Delta})$. Comme $Cl(\Delta)$ est naturellement un groupe, cette bijection donne une structure de groupe à $\mathcal{F}(\Delta)$. En transportant de $Cl(\Delta)$ à $\mathcal{F}(\Delta)$ les formules de multiplication des idéaux, on trouve les formules de Dirichlet pour la composition des formes quadratiques.

Nous avons donc trois points de vue différents pour la composition dans le groupe $Cl(\Delta)$. Nous allons montrer que le théorème 2.2 permet de calculer des racines carrées dans le groupe de classes $Cl(\Delta)$, c'est–à–dire, à partir d'une forme primitive Q de discriminant Δ, de trouver une autre forme primitive R de discriminant Δ telle que $[R]^2 = [Q]$ dans $Cl(\Delta)$.

Notons $Q(s,t) = As^2+Bst+Ct^2$ et $R(s,t) = as^2+bst+ct^2$ deux formes quadratiques de discriminant Δ. Notons aussi $Q = \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}$. En utilisant la définition originale de Gauss pour la composition (voir [6, §235] ou [1, §2.5]), on a la définition suivante pour la duplication :

Définition (duplication d'une forme quadratique)**.** Soient R et Q deux formes quadratiques binaires primitives de discriminant Δ. On dit que $[R]^2 = [Q]$ si l'on peut trouver des entiers $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ tels que l'on ait la relation

$$(1)\quad R(s_1,t_1)R(s_2,t_2) = Q(x_1s_1s_2 + x_2s_1t_2 + x_3t_1s_2 + x_4t_1t_2, \\ y_1s_1s_2 + y_2s_1t_2 + y_3t_1s_2 + y_4t_1t_2) ,$$

avec la condition d'orientation donnée par

$$x_1y_2 - y_1x_2 = x_1y_3 - y_1x_3 = R(1,0)\ . \tag{2}$$

Lemme 4.1 (définition simplifiée de la duplication)**.** *Soient R et Q deux formes quadratiques binaires primitives de discriminant Δ non carré. On a $[R]^2 = [Q]$ dans $Cl(\Delta)$ si et seulement si l'on peut trouver des entiers $x_1, x_2, x_4, y_1, y_2, y_4$ tels que l'on ait les relations*

$$\begin{aligned} R(s_1,t_1)R(s_2,t_2) = Q(&x_1s_1s_2 + x_2s_1t_2 + x_2t_1s_2 + x_4t_1t_2,\\ &y_1s_1s_2 + y_2s_1t_2 + y_2t_1s_2 + y_4t_1t_2)\ , \end{aligned} \tag{3}$$

et

$$x_1y_2 - y_1x_2 = R(1,0)\ . \tag{4}$$

Démonstration. Il suffit de montrer que les relations (1) et (2) ne peuvent être vérifiées que si $x_2 = x_3$ et $y_2 = y_3$. Notons $X_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$, pour $i = 1, \ldots, 4$. En identifiant les coefficients dans (1), on voit que la relation (1) équivaut aux relations

$$\begin{cases} X_1^tQX_1 = a^2 \\ X_4^tQX_4 = c^2 \\ 2X_3^tQX_4 = 2X_2^tQX_4 = bc \\ 2X_3^tQX_1 = 2X_2^tQX_1 = ab \\ X_2^tQX_2 = X_3^tQX_3 = ac \\ 2X_2^tQX_3 + 2X_1^tQX_4 = b^2 \end{cases}$$

et la relation (2) équivaut à

$$\det(X_1, X_2) = \det(X_1, X_3) = a\ .$$

Montrons que l'on a $X_2 = X_3$. Puisque Δ n'est pas un carré, a ne peut pas être nul, et donc $X_1 \neq 0$. On a $\det(X_1, X_2 - X_3) = 0$, donc $X_2 - X_3$ est de la forme $X_2 - X_3 = \lambda X_1$. On a aussi $2(X_2 - X_3)^tQX_1 = 0$. De là, on déduit $\lambda a^2 = 0$, donc $\lambda = 0$ et $X_2 = X_3$. □

Lemme 4.2. *Soient R et Q deux formes quadratiques primitives de discriminant Δ. La relation (3) équivaut à $[R]^2 = [Q]^{\pm 1}$ dans $Cl(\Delta)$.*

Démonstration. Par définition, $[Q(s,t)]^{-1} = [Q(-s,t)]$, il est donc clair d'après le lemme 4.1 que la relation $[R]^2 = [Q]^{\pm 1}$ implique (3). Pour la réciproque, il suffit de voir que (3) implique (4) au signe près. Utilisons les

notations du lemme 4.1. La relation (3) équivaut aux relations

$$(5)\qquad \begin{cases} X_1^t Q X_1 = a^2 \\ X_4^t Q X_4 = c^2 \\ 2X_2^t Q X_4 = bc \\ 2X_2^t Q X_1 = ab \\ X_2^t Q X_2 = ac \\ 2X_1^t Q X_4 = b^2 - 2ac \end{cases}$$

Le déterminant de la matrice de Q dans la base X_1, X_2 donne

$$\Delta \det(X_1, X_2)^2 = -4\left((X_1^t Q X_1)(X_2^t Q X_2) - (X_1^t Q X_2)^2\right) .$$

En simplifiant par $\Delta \neq 0$, on trouve $\det(X_1, X_2)^2 = a^2$. □

Théorème 4.3. *Soient Q et R deux formes quadratiques entières primitives de discriminant Δ (non carré). Les propositions suivantes sont équivalentes :*

(i) on a $[R]^2 = [Q]^{\pm 1}$ dans $Cl(\Delta)$,

(ii) on peut trouver deux formes quadratiques entières $x(s,t) = x_1 s^2 + 2x_2 st + x_4 t^2$ et $y(s,t) = y_1 s^2 + 2y_2 st + y_4 t^2$ (avec x_2 et $y_2 \in \mathbb{Z}$), telles que les solutions de $Q(X,Y) = 1$ soient paramétrées par $X = \dfrac{x(s,t)}{R(s,t)}$ et $Y = \dfrac{y(s,t)}{R(s,t)}$.

(iii) on peut trouver deux formes quadratiques entières $x(s,t) = x_1 s^2 + 2x_2 st + x_4 t^2$ et $y(s,t) = y_1 s^2 + 2y_2 st + y_4 t^2$ (avec x_2 et $y_2 \in \mathbb{Z}$), non proportionnelles, telles que $Q(x,y) = R(s,t)^2$.

Remarque. Dans la condition (ii), si l'on change x en $-x$, on obtient une paramétrisation des solutions de $Q(-X,Y) = 1$. Comme $Q(-s,t)$ est l'inverse de $Q(s,t)$ pour la composition des formes quadratiques, cela justifie l'apparition de l'exposant ± 1 dans (i). Il n'est pas difficile de rajouter une condition de signe sur x pour obtenir exactement $[R]^2 = [Q]$ dans (i). Dans la condition (iii), la non–proportionnalité des formes quadratiques sert à éviter la solution triviale $Q(x_0 R, y_0 R) = R^2$, où $Q(x_0, y_0) = 1$.

Démonstration. (ii) ⇔ (iii). On applique la proposition 1.3.

(i) ⇒ (ii). Il suffit de prendre $s_1 = s_2 = s$ et $t_1 = t_2 = t$ dans la relation (3) et d'appliquer le lemme 4.2.

(iii) ⇒ (i). Soit $\mathfrak{Q} = \begin{pmatrix} A & \frac{B}{2} & 0 \\ \frac{B}{2} & C & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Le déterminant de $\mathfrak{Q}$ vaut $\det \mathfrak{Q} = \frac{\Delta}{4}$. Soit $q = \begin{pmatrix} x_1 & 2x_2 & x_4 \\ y_1 & 2y_2 & y_4 \\ a & b & c \end{pmatrix}$. Puisque x et y ne sont pas proportionnelles,

alors $\operatorname{Rang} q > 1$. Comme, de plus, $\mathfrak{Q}(x, y, R) = 0$, d'après la proposition 1.4, on a $\operatorname{Disc} R = \Delta\mu^2$. Mais par hypothèse, $\operatorname{Disc} R = \Delta$, donc $\mu^2 = 1$. On a alors

$$q^t \mathfrak{Q} q = -\Delta \mathfrak{Q}_0 \, . \tag{6}$$

Montrons les formules (5).

Le coefficient $(1,1)$ de (6) donne $X_1^t Q X_1 - a^2 = 0$.

Le coefficient $(3,3)$ de (6) donne $X_4^t Q X_4 - c^2 = 0$.

Le coefficient $(2,3)$ de (6) donne $2X_2^t Q X_4 - bc = 0$.

Le coefficient $(1,2)$ de (6) donne $2X_1^t Q X_2 - ab = 0$.

Le coefficient $(2,2)$ de (6) donne $4X_2^t Q X_2 - b^2 = -\Delta$, donc $X_2^t Q X_2 = ac$.

Le coefficient $(1,3)$ de (6) donne $X_1^t Q X_4 - ac = \frac{\Delta}{2}$, donc $2X_1^t Q X_4 = b^2 - 2ac$.

La relation (3) est donc vérifiée. D'après le lemme 4.2, on a $[R]^2 = [Q]^{\pm 1}$. □

5. Primitivité de la paramétrisation

Lorsque l'on veut résoudre l'équation $[R]^2 = [Q]^{\pm 1}$ dans $Cl(\Delta)$ à l'aide du théorème 4.3, on peut utiliser la paramétrisation des solutions de $Q(X, Y) = Z^2$ donnée par le corollaire 2.3, à condition que cette paramétrisation soit primitive. Nous examinons ici les conditions de primitivité de cette paramétrisation à partir de la solution particulière utilisée.

Proposition 5.1. *Soit $Q = as^2 + bst + ct^2$ une forme quadratique entière de discriminant $\Delta \neq 0$ et D un entier non nul. Soit $\mathfrak{Q} = \begin{pmatrix} A & \frac{B}{2} & 0 \\ \frac{B}{2} & C & 0 \\ 0 & 0 & -D \end{pmatrix}$. Soit $X_0 = (x_1, x_2, x_3)$ une solution particulière entière primitive de $\mathfrak{Q}(x_1, x_2, x_3) = 0$ et soit (q_1, q_2, q_3) la paramétrisation construite dans le corollaire 2.3. Soit p un entier $p \geqslant 1$. Si $p \mid q_3$, alors $p^2 \mid \Delta$ et Δp^{-2} est le discriminant d'une forme quadratique binaire.*

En particulier, lorsque Δ est un discriminant fondamental, q_3 est toujours primitive.

Démonstration. Ceci est évident d'après le corollaire 2.3. □

Proposition 5.2. *Sous les mêmes hypothèses que la proposition 5.1, on suppose de plus que Q est primitive et que p est un nombre premier vérifiant*

$$p^2 \mid \Delta, \text{ et } p^2 \nmid D \, ,$$

(lorsque $p = 2$, on suppose seulement $p^2 \mid \Delta$), alors on a

$$p \mid q_3 \Longleftrightarrow p \mid x_3 \, .$$

Démonstration. Commençons par le cas $p \neq 2$.

$\Leftarrow$: Quitte à faire un changement de variables en s et t, on peut supposer que $p \mid a$. Comme $p^2 \mid \Delta$, on a $p \mid b$, $p^2 \mid a$ et $p \nmid c$ (car Q est primitive). La solution particulière vérifie alors $cx_2^2 = Dx_3^2 \mod p$, et comme $p \mid x_3$, on a aussi $p \mid x_2$, et $p \nmid x_1$ (car X_0 est primitif). En regardant la réduction modulo p de M et $\mathfrak{Q}$, on voit que $\mathfrak{Q}' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & c' & \frac{d'}{2} \\ 0 & \frac{d'}{2} & e' \end{pmatrix} \mod p$ donc $\widehat{\mathfrak{Q}'} = \begin{pmatrix} c' & d' & e' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mod p$, et enfin $q = M\widehat{\mathfrak{Q}'} = \begin{pmatrix} x_1c' & x_1d' & x_1e' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mod p$. Donc $p \mid q_3$.

$\Rightarrow$: On peut, comme précédemment, supposer que $p^2 \mid a$, $p \mid b$, $p \nmid c$. La paramétrisation donne $cq_2^2 = 0 \mod p$, donc $p \mid q_2$. Ainsi, le rang sur $\mathbb{F}_p$ de $q = M\widehat{\mathfrak{Q}'}$ est au plus 1. Il ne peut pas être nul car q_1 n'est pas divisible par p (son discriminant est $-4c$), donc le rang est 1. Comme $\det M = 1$, le rang de $\widehat{\mathfrak{Q}'}$ est aussi égal à 1. Soit $\mathfrak{Q}' = \begin{pmatrix} 0 & \frac{a'}{2} & \frac{b'}{2} \\ \frac{a'}{2} & c' & \frac{d'}{2} \\ \frac{b'}{2} & \frac{d'}{2} & e' \end{pmatrix}$ et $\widehat{\mathfrak{Q}'} = \begin{pmatrix} c' & d' & e' \\ -a' & -b' & 0 \\ 0 & -a' & -b' \end{pmatrix}$. Le rang sur $\mathbb{F}_p$ de $\widehat{\mathfrak{Q}'}$ n'étant que 1, on doit avoir $a' = b' = 0 \mod p$. Mais alors $\mathfrak{Q}' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & c' & \frac{d'}{2} \\ 0 & \frac{d'}{2} & e' \end{pmatrix} \mod p$, donc X_0 est dans le noyau de $\mathfrak{Q}$ mod p. En particulier, $cx_2 = 0 \mod p$, donc $p \mid x_2$. En regardant la relation $\mathfrak{Q}(x_1, x_2, x_3) = 0$ modulo p^2, on trouve alors $Dx_3^2 = 0 \mod p^2$, mais $p^2 \nmid D$, donc $p \mid x_3$.

Pour le cas $p = 2$, on commence par regarder la condition $4 \mid \Delta$. Sous cette condition, on a $2 \mid b$, et donc les matrices $\mathfrak{Q}$ et $\mathfrak{Q}'$ sont dans $\mathcal{M}_3(\mathbb{Z})$. Soit $\mathfrak{Q}' = \begin{pmatrix} 0 & a' & b' \\ a' & c' & d' \\ b' & d' & e' \end{pmatrix}$. On a alors $\widehat{\mathfrak{Q}'} = \begin{pmatrix} c' & 0 & e' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mod 2$, et donc $q_3 = x_3(c's^2 + e't^2) \mod 2$. Mais Q est primitive, donc la forme quadratique $\mathfrak{Q}$ est impaire (il existe au moins un coefficient impair sur la diagonale), ainsi que $\mathfrak{Q}'$, et donc l'un au moins des coeffficients c' ou e' est impair. A partir de là, il est facile de voir que $2 \mid q_3$ si et seulement si $2 \mid x_3$. □

6. Comparaison avec l'algorithme de Gauss

Supposons que l'on ait une forme quadratique primitive Q de discriminant Δ, et que l'on sache que cette forme soit dans le genre principal. Si Δ est un discriminant fondamental, alors pour chercher une solution de

$[R]^2 = [Q]^{\pm 1}$, il suffit d'après le théorème 4.3 et la proposition 5.1 de trouver une solution particulière de $Q(X,Y) = 1$, par exemple à l'aide de [11], et d'en déduire une paramétrisation de toutes les solutions à l'aide du corollaire 2.3 et de la construction du théorème 2.2 : la forme R est donnée par q_3.

Lorsque Δ n'est plus fondamental, on écrit $\Delta = \Delta_0 f^2$, où Δ_0 est un discriminant fondamental, il faut alors s'assurer en plus que la solution particulière de $Q(x_1, x_2) = x_3^2$ soit telle que x_3 est premier à f (d'après la proposition 5.2). Cette remarque éclaire le travail réalisé dans [6] et [7] pour trouver une solution entière de certaines équations quadratiques ayant de bonnes propriétés de divisibilité. On voit ici que ce travail n'est pas nécessaire lorsque Δ est un discriminant fondamental.

Comparons notre algorithme de résolution de $[R]^2 = [Q]^{\pm 1}$ dans $Cl(\Delta)$ et celui de Gauss, décrit dans [6, §286], [8] et [1]. Nous allons constater que celui de Gauss est essentiellement identique au nôtre, mais qu'il utilise des propriétés spécifiques à cette situation pour être un peu plus efficace. Afin d'effectuer cette comparaison, on se place dans le cas particulier où $Q = AX^2+BXY+CY^2 = AX^2+2B'XY+CY^2$ est une forme quadratique primitive de discriminant $\Delta = 4(B'^2-AC)$, et où l'on suppose que $\Delta' = \frac{1}{4}\Delta$ est sans facteur carré (et différent de 0 et 1). Par symétrie des coefficients A et C, on suppose que A est impair lorsque Δ' est pair (ce qui assurera la primitivité de la solution trouvée).

Les grandes étapes de l'algorithme de Gauss sont les suivantes :

1- Construire une matrice symétrique Q de déterminant -1 et de la forme

$$\mathfrak{Q}' = \begin{pmatrix} A & B' & * \\ B' & C & * \\ * & * & * \end{pmatrix}.$$

2- Trouver une matrice unimodulaire B telle que

$$B^t \mathfrak{Q}' B = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \quad :$$

la solution est donnée par la dernière ligne de B.

En combinant le théorème 2.2 et la résolution des équations quadratiques ternaires de [11], notre algorithme est le suivant :

1-*Recherche d'une solution particulière*

1a- On considère la matrice $\mathfrak{Q} = \begin{pmatrix} A & B' & 0 \\ B' & C & 0 \\ 0 & 0 & -1 \end{pmatrix}$. On cherche une matrice $V \in \mathcal{M}_3(\mathbb{Z})$ de déterminant $\det V = \Delta'$ telle que

$V^t\mathfrak{Q}V = -\Delta'\mathfrak{Q}'$ où la matrice $\mathfrak{Q}'$ a des coefficients entiers et $\det \mathfrak{Q}' = -1$ (par exemple en utilisant [11]).

1b- On réduit la matrice $\mathfrak{Q}'$ pour trouver $B \in SL_3(\mathbb{Z})$ telle que $B^t\mathfrak{Q}'B = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$ (par exemple en utilisant [11]).

1c- On considère la solution particulière X_0 donnée par la première colonne de la matrice VB.

2- *Construction de la paramétrisation*

2a- On construit une matrice $M \in SL_3(\mathbb{Z})$ dont la première colonne soit X_0 (voir théorème 2.2).

2b- On pose $\mathfrak{Q}'' = M^t\mathfrak{Q}'M$, Alors la matrice $q = M\widehat{\mathfrak{Q}''}$ (voir lemme 1.3) satisfait $q^t\mathfrak{Q}q = (-4\det\mathfrak{Q})\mathfrak{Q}_0$ et $\det q = -4\det\mathfrak{Q}$.

2c- D'après le thèorème 2.2 et le théorème 4.3, la dernière ligne de q contient les coefficients de la forme quadratique R cherchée.

Pour écrire cet algorithme, on a utilisé différents algorithmes généraux. Mais pour cette application particulière, on peut proposer des amélioriations. La première amélioration évidente que l'on peut faire est de remarquer que l'on peut entièrement remplacer l'étape 2 par $q = VB\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$,

La deuxième amélioration concerne la construction de la matrice V de l'étape 1a. En effet, plutôt que d'utiliser la méthode générale de [11], on peut remarquer que l'on peut choisir V de la forme

$$V = \begin{pmatrix} C & -B' & a_1 \\ -B' & A & a_2 \\ 0 & 0 & -1 \end{pmatrix},$$

à condition que a_1 et a_2 satisfassent la relation

$$Aa_1^2 + 2B'a_1a_2 + Ca_1^2 \equiv 1 \mod \Delta'.$$

La matrice $\mathfrak{Q}'$ de déterminant -1 est alors de la forme

$$\mathfrak{Q}' = \begin{pmatrix} C & -B' & a_1 \\ -B' & A & a_2 \\ a_1 & a_2 & * \end{pmatrix}.$$

En utilisant ces deux remarques, on obtient une description des formes quadratiques dans le genre principal très proche de celle de Gauss, comme elle est décrite dans [1, Th. 6.7]. En particulier, une forme quadratique binaire est dans le genre principal, lorsque l'on peut la compléter en une forme quadratique ternaire de déterminant -1. L'algorithme de Gauss consiste donc à construire directement cette matrice $\mathfrak{Q}'$.

Lorsque la forme quadratique $Q = AX^2 + 2B'XY + CY^2$ est réduite, ses coefficients sont de l'ordre de $\Delta^{1/2}$. Expérimentalement, on constate que lorsque la matrice $\mathfrak{Q}'$ est construite à l'aide de la méthode générale [11], elle a des coefficients de la taille de $\Delta^{5/2}$, alors qu'avec cette amélioration ils ne sont plus que de l'ordre de $\Delta^{3/2}$, lorsque l'on choisit a_1 et a_2 entre $-\frac{\Delta'}{2}$ et $\frac{\Delta'}{2}$.

Mais la méthode de Gauss pour construire cette matrice $\mathfrak{Q}'$ est encore légèrement différente. Plutôt que de construire directement les coefficients a_1 et a_2, il construit la matrice adjointe $\mathfrak{Q}'^*$ (voir [1, Lemma. 6.1]). En identifiant les coefficients, cela revient à trouver les coefficients $m = (\mathfrak{Q}^*)_{1,3}$ et $n = (\mathfrak{Q}^*)_{2,3}$ satisfaisant les relations

$$m^2 \equiv c \mod \Delta' \quad mn \equiv b \mod \Delta' \quad n^2 \equiv a \mod \Delta' .$$

Lorsque l'on choisit m et n entre $-\frac{\Delta'}{2}$ et $\frac{\Delta'}{2}$, on constate (expérimentalement encore) que les coefficients de $\mathfrak{Q}'$ ne sont plus que de l'ordre de $\Delta^{1/2}$.

On constate donc que la méthode de Gauss repose exactement sur les mêmes relations que notre algorithme, mais que dans la pratique sa construction de la matrice $\mathfrak{Q}'$ donne des coefficients beaucoup plus petits, et donc la réduction de l'étape suivante est beaucoup plus rapide. Cette différence constatée expérimentalement vient évidemment du fait que la matrice construite ici a des propriétés particulières (la taille de la matrice n'est que de 3 et certains de ses coefficients sont connus !), que ne peut pas utiliser l'algorithme général de [11]. Toutefois, cela suggère qu'il est possible d'améliorer cet algorithme de minimisation pour qu'il construise des matrices ayant des coefficients plus petits. Il serait tout à fait intéressant d'obtenir une telle amélioration.

Les résultats de ce papier permettent donc de donner une nouvelle interprétation de l'algorithme de Gauss, en reliant le problème technique de la racine carrée dans le groupe de classes à celui beaucoup plus classique de la paramétrisation des solutions d'une équation quadratique, en particulier pour l'existence d'une matrice symétrique unimodulaire ayant certains coefficients fixés, et pour la construction de la solution à partir de cette matrice.

Références

[1] W. BOSMA, P. STEVENHAGEN, *On the computation of quadratic 2-class groups*. J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313.

[2] J.W.S. CASSELS, *Rational Quadratic Forms*. L.M.S. Monographs, Academic Press (1978).

[3] H. COHEN, *A Course in Computational Algebraic Number Theory*. Graduate Texts in Math. **138**, Third corrected printing, Springer–Verlag (1996).

[4] D. COX, Primes of the form $x^2 + ny^2$, Fermat, class field theory, and complex multiplication. Wiley–Interscience (1989).

[5] J. Cremona, D. Rusin, *Efficient solution of rational conics*. Math. Comp. **72** (2003), 1417–1441.

[6] K.F. Gauss, *Recherches Arithmétiques*. Poullet-Delisle, A.C.M. (trad.), A. Blanchard, 1953.

[7] K. Hardy, K. Williams, *The squareroot of an ambiguous form in the principal genus*. Proc. Edinburgh Math. Soc. (2) **36** (1993), no. 1, 145–150.

[8] J.C. Lagarias, *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*. J. Ameri. Math. Soc. **2** (1989), no 4, 143–186.

[9] D. Shanks, *Gauss's ternary form reduction and the* 2*-Sylow subgroup*. Math. Comp. **25**, no 116 (1971), 837–853 ; Erratum : Math. Comp. **32** (1978), 1328–1329.

[10] D. Simon, *Computing the rank of elliptic curves over number fields*. London Math. Soc. Journal of Computation and Mathematics, vol **5** (2002) 7–17.

[11] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms*. Math. Comp. **74**, no 251 (2005), 1531–1543.

[12] N.P. Smart, *The algorithmic resolution of Diophantine equations*. London Math. Soc. Student Texts **41**, Cambridge University Press, 1998.

Denis Simon
LMNO - UMR 6139
Université de Caen – France
Campus II – Boulevard Mal Juin
BP 5186 – 14032 Caen Cedex, France
E-mail: simon@math.unicaen.fr